(D) Include an annual review of each program to determine whether it continues to meet the requirements of the Order.

(iii) Assess whether:

(A) Senior management demonstrates commitment to the success of the program, including providing the necessary resources for effective implementation;

(B) Producers and users of classified information receive guidance with respect to security responsibilities and requirements;

(C) Controls to prevent unauthorized access to classified information are effective;

(D) Contingency plans are in place for safeguarding classified information used in or near hostile areas;

(E) The performance contract or other system used to rate civilian or military personnel includes the management of classified information as a critical element or item to be evaluated in the rating of: Original classifiers; security managers; classification management officers; and security specialists; and other employees whose duties significantly involve the creation or handling of classified information; and

(F) A method is in place for collecting information on the costs associated with the implementation of the Order.

Subpart F—Security Education and Training

§ 2001.70 General [5.4].

(a) *Purpose*. This subpart sets standards for agency security education and training programs. Implementation of these standards should:

(1) Ensure that all executive branch employees who create, process or handle classified information have a satisfactory knowledge and understanding about classification, safeguarding, and declassification policies and procedures;

(2) Increase uniformity in the conduct of agency security education and training programs; and

(3) Reduce improper classification, safeguarding and declassification practices.

(b) *Applicability*. These standards are binding on all executive branch departments and agencies that create or handle classified information. Pursuant to Executive Order 12829, the NISPOM prescribes the security requirements, restrictions, and safeguards applicable to industry, including the conduct of contractor security education and training. The standards established in the NISPOM should be consistent with the standards prescribed in Executive Order 12958, as amended and of this part.

(c) *Responsibility*. The senior agency official is responsible for the agency's security education and training program. The senior agency official shall designate agency personnel to assist in carrying out this responsibility.

(d) *Approach*. Security education and training should be tailored to meet the specific needs of the agency's security program, and the specific roles employees are expected to play in that program. The agency official(s) responsible for the program shall determine the means and methods for providing security education and training. Training methods may include briefings, interactive videos, dissemination of instructional materials, and other media and methods. Agencies shall maintain records about the programs it has offered and employee participation in them.

(e) *Frequency*. The frequency of agency security education and training will vary in accordance with the needs of the agency's security classification program. Each agency shall provide some form of refresher security education and training at least annually.

§ 2001.71 Coverage [5.4(d)(3)].

(a) *General*. Each department or agency shall establish and maintain a formal security education and training program which provides for initial and refresher training, and termination briefings. This subpart establishes security education and training standards for original classification authorities, declassification authorities, security managers, classification management officers, security specialists, and all other personnel whose duties significantly involve the creation or handling of classified information. These

standards are not intended to be all-inclusive. The official responsible for the security education and training program may expand or modify the coverage provided in this part according to the agency's program and policy needs.

(b) *Elements of initial coverage.* All cleared agency personnel shall receive initial training on basic security policies, principles, practices, and criminal, civil, and administrative penalties. Such training must be provided in conjunction with the granting of a security clearance, and prior to granting access to classified information. The following areas should be considered for inclusion in initial briefings.

(1) Roles and responsibilities.

(i) What are the responsibilities of the senior agency official, classification management officers, the security manager and the security specialist?

(ii) What are the responsibilities of agency employees who create or handle classified information?

(iii) Who should be contacted in case of questions or concerns about classification matters?

(2) Elements of classifying and declassifying information.

(i) What is classified information and why is it important to protect it?

(ii) What are the levels of classified information and the damage criteria associated with each level?

(iii) What are the prescribed classification markings and why is it important to have classified information fully and properly marked?

(iv) What are the general requirements for declassifying information?

(v) What are the procedures for challenging the classification status of information?

(3) Elements of safeguarding.

(i) What are the proper procedures for safeguarding classified information?

(ii) What constitutes an unauthorized disclosure and what are the criminal, civil, and administrative penalties associated with these disclosures?

(iii) What are the general conditions and restrictions for access to classified information?

(iv) What should an individual do when he or she believes safeguarding standards may have been violated?

(c) *Specialized security education and training.* Original classification authorities, authorized declassification authorities, individuals specifically designated as responsible for derivative classification, classification management officers, security managers, security specialists, and all other personnel whose duties significantly involve the creation or handling of classified information should receive more detailed training. This training should be provided before or concurrent with the date the employee assumes any of the positions listed above, but in any event no later than six months from that date. Coverage considerations should include:

(1) Original Classification Authorities.

(i) What is the difference between original and derivative classification?

(ii) Who can classify information originally?

(iii) What are the standards that a designated classifier must meet to classify information?

(iv) What discretion does the Original Classification Authority have in classifying information, for example, foreign government information.

(v) What is the process for determining duration of classification?

(vi) What are the prohibitions and limitations on classifying information?

(vii) What are the basic markings that must appear on classified information?

(viii) What are the general standards and procedures for declassification?

(2) Declassification authorities other than original classification authorities.

(i) What are the standards, methods and procedures for declassifying information under Executive Order 12958, as amended?

(ii) What are the standards for creating and using agency declassification guides?

(iii) What is contained in the agency's automatic declassification plan?

(iv) What are the agency responsibilities for the maintenance of a declassification database?

(3) Individuals specifically designated as responsible for derivative classification, security managers, classification

management officers, security specialists or any other personnel whose duties significantly involve the creation or handling of classified information.

(i) What are the original and derivative classification processes and the standards applicable to each?

(ii) What are the proper and complete classification markings, as described in subpart B of this part?

(iii) What are the authorities, methods and processes for downgrading and declassifying information?

(iv) What are the methods for the proper use, storage, reproduction, transmission, dissemination and destruction of classified information?

(v) What are the requirements for creating and updating classification and declassification guides?

(vi) What are the requirements for controlling access to classified information?

(vii) What are the procedures for investigating and reporting instances of security violations, and the penalties associated with such violations?

(viii) What are the requirements for creating, maintaining, and terminating special access programs, and the mechanisms for monitoring such programs?

(ix) What are the procedures for the secure use, certification and accreditation of automated information systems and networks which use, process, store, reproduce, or transmit classified information?

(x) What are the requirements for oversight of the security classification program, including agency self-inspections?

(d) *Refresher security education and training.* Agencies shall provide refresher training to employees who create, process or handle classified information. Refresher training should reinforce the policies, principles and procedures covered in initial and specialized training. Refresher training should also address the threat and the techniques employed by foreign intelligence activities attempting to obtain classified information, and advise personnel of penalties for engaging in espionage activities. Refresher training should also address issues or concerns identified during agency self-inspections. When other methods are impractical, agencies may satisfy the requirement for refresher training by means of audiovisual products or written materials.

(e) *Termination briefings.* Each agency shall ensure that each employee granted access to classified information who leaves the service of the agency receives a termination briefing. Also, each agency employee whose clearance is withdrawn must receive such a briefing. At a minimum, termination briefings must impress upon each employee: The continuing responsibility not to disclose any classified information to which the employee had access and the potential penalties for non-compliance; and the obligation to return to the appropriate agency official all classified documents and materials in the employee's possession.

(f) *Other security education and training.* Agencies are encouraged to develop additional security education and training according to program and policy needs. Such security education and training could include:

(1) Practices applicable to U.S. officials traveling overseas;

(2) Procedures for protecting classified information processed and stored in automated information systems;

(3) Methods for dealing with uncleared personnel who work in proximity to classified information;

(4) Responsibilities of personnel serving as couriers of classified information; and

(5) Security requirements that govern participation in international programs.

Subpart G—Reporting and Definitions

§ 2001.80 Statistical reporting [5.2(b)(4)].

Each agency that creates or handles classified information shall report annually to the Director of ISOO statistics related to its security classification program. The Director will instruct agencies what data elements are required, and how and when they are to be reported.

§ 2001.81 Accounting for costs [5.4(d)(8)].

(a) Information on the costs associated with the implementation of the